HAYNES BOONE

August 17, 2022

A New Guideline Added to China's Data Protection Framework

By Liza L.S. Mark, Sarah Sheng

The *Security Assessment Measures for Data Export* (《数据出境安全评估办法》, hereinafter as "***Measures***") were recently released by the Cyberspace Administration of China ("***CAC***"), and will become effective September 1, 2022. The Measures further define the requirement of security assessment by the government for outbound data transfers, as further defined below ("***Data Export***") under the regime of China's Data Laws ("***Data Protection Laws***")[1] and provide a preliminary reference for multinational companies ("***MNCs***") to prepare and carry out internal controls for data related operations. Here is a brief overview of the Measures. The data and personal information discussed in this article refer to such information collected and generated in China.

1. Application Scope

- The situations where a declaration to the CAC for security assessment for data export through the local provincial cyberspace administration authority is required include:
    - Where a "Data Processor"[2] exports "Critical Data"[3] abroad;
    - Where a "Critical Information Infrastructure Operator"[4] ("***CIIO***") or a "Data Processor" which processes "personal information"[5] ("***PI***") of more than 1 million individuals, exports personal information abroad;

[1] ***Personal Information Protection Law*** (《个人信息保护法》), effective November 1, 2021; the Data Security Law (《数据安全法》), effective September 1, 2021; and the ***Cybersecurity Law*** (《网络安全法》), effective June 1, 2017, collectively as "***Data Laws***."

[2] "***Data Processor***": those who collect, store, use, process, transmit, provide and publicize data. ***Article 3, Data Security Law***.

[3] "***Critical Data***" refers to the data that, once tampered with, destroyed, leaked, illegally obtained or illegally used, may endanger national security, economic operation, social stability, public health and security, etc. ***Article 19, the Measures***.

[4] Critical Information Infrastructure Operator ("***CIIO***"): those that construct, operate, maintain and/or use a network in China, involved with critical information infrastructure. ***Article 31, Article 76, Cybersecurity Law***.

[5] "Personal Information" ("***PI***"): means all types of information relating to identified or identifiable individuals that is recorded by electronic or other means, excluding anonymously processed information. ***Article 4, Personal Information Protection Law.***

- Where a "Data Processor" has exported abroad PI of 100,000 individuals or "Sensitive PI"[6] of 10,000 individuals in total since January 1 of the previous year; and

- Other data export situations prescribed by the CAC.

- What constitutes "Data Export?"

  According to the CAC at the press conference announcing the Measures, "Data Export" includes:

  - Transportation or storage of the data abroad (i.e., out of Mainland China); and

  - Providing agencies, organizations and individuals outside of China with access to the data stored in China.

  There is no clear definition of what other exposures would be considered "data export," but providing access to data within China to a foreign national in circumvention of the intention of the Data Protection Laws and the Measures may also be considered "Data Export."

2. The Requirements of Self-assessment and Security Assessment

The Measures require the Data Processor to first conduct a self-assessment on the risks of Data Export before application for official Security Assessment with the CAC. The main considerations for both the self-assessment and the CAC Security Assessment include:

	Self-assessment:	**Security Assessment**
Procedure	- To be conducted by the company itself - The assessment report needs to be filed as part of the application for the official Security Assessment with CAC	- Filing application through the local provincial cyberspace administration authority to the CAC (5 working days for the local authority to check the completeness of the application documents) - CAC shall decide whether to accept the application after receipt of the application documents (7 working days to check and notify the applicant) - CAC will organize the Security Assessment with other relevant departments of the State Council after accepting the application (to be completed in 45 working days after the

[6] "***Sensitive PI***": those PI that is likely to result in damage to the personal dignity, personal safety or property safely of any individual once leaked or illegally used, including such information as biometric identification, religious belief, specific identity, medical health, financial account and whereabouts and tracks, as well as the PI of minors under the age of 14. ***Article 28, Personal Information Protection Law***.

© 2022 Haynes and Boone, LLP

		application is accepted, may be extended in case of complicated situations and supplementary materials required)
Assessment Factors	- the legality, legitimacy and necessity of the purpose, scope and method of the Data Export and data processing by the overseas recipient; - the scale, scope, type and sensitivity of the data to be provided abroad, and the risks to national security, public interests or the legitimate rights and interests of individuals or organizations caused by the Data Export; - the responsibilities and obligations that the overseas recipient promises to undertake, and whether the overseas recipient's management and technical measures and capabilities for performing its responsibilities and obligations can guarantee the security of the Data Export; - risks of the data being tampered with, destroyed, divulged, lost, transferred, illegally obtained or illegally used during and after the Data Export; whether the protections for the maintenance of personal information rights and interests is viable; - whether the relevant contracts on the Data Export to be concluded with the overseas recipient or other legally binding documents ("***Legal Documents***") fully cover the responsibilities and obligations to protect the data security; and - other matters that may affect the security of the Data Exported	- the legality, legitimacy and necessity of the purpose, scope, and method of the Data Export; - the impact of the data security protection policies and regulations and the cybersecurity environment of the country or region where the overseas recipient is located on the security of data to be exported, and whether the data protection level of the overseas recipient meets the requirements of China's applicable laws and regulations and mandatory national standards; - the size, scope, types and sensitivity of data to be provided abroad, and the risks that the data may be tampered with, destroyed, divulged, lost, transferred, illegally obtained or illegally used during and after the data is exported; - whether data security and personal information rights and interests can be fully and effectively guaranteed; - whether the Legal Documents to be concluded by the Data Processor and the overseas recipient fully cover the responsibilities and obligations of data security protection; - compliance with China's applicable laws and regulations; and - other matters that the CAC considers necessary to assess.

3. Some Key Timing Points

- **2 years**: once a Security Assessment confirmation is granted, it will be valid for 2 years from date of issuance.

    - If any factor affecting the security of the Exported Data changes during the period of validity, such as the purpose, method, scope, type of the Exported Data and the security protection policies in

© 2022 Haynes and Boone, LLP

the region where the overseas recipient located are change, the Data Processor will need to process a new Security Assessment.

- If the Security Assessment confirmation will expire while Data Export is still ongoing, the Data Processor must file a new Security Assessment 60 working days prior to the expiration.

- **6 months**: the Measures will take effect as of September 1, 2022. Any Data Export that is not in compliance with the Measures must be rectified within 6 months from September 1, 2022.

There is still a great deal of uncertainty on where the exact limitations are, but the Measures are one of the first solid areas for guidance on implementation of the Data Protection Laws. Therefore, if MNCs have not already, they must take action to (i) categorize the data they collect and generate in China; (ii) reconsider the data that needs to be exported; (iii) identify the situations where a Data Export Security Assessment application is required; (iv) prepare the self-assessment of any expected Export Data, particularly putting in place any Legal documents with the overseas recipients that is required; (v) coordinate with overseas recipients to prepare necessary information for assessment, e.g. security measure, statement on local data protection capabilities where the recipients are located, etc.; and (vi) apply for the Security Assessment with the CAC if necessary.

For more information, please visit our China Updates page or see the following resources:

China Revises its Anti-Monopoly Law 14 Years After its Initial Implementation, July 26, 2022

China Releases Judicial Interpretation of Anti-Unfair Competition Law, April 28, 2022

Select Proposed Changes to the Company Law of the People's Republic of China, March 22, 2022

A Snapshot of China's Cyberspace Administration and Data Protection Framework, February 9, 2022

China Intensifies Regulations on Cryptocurrency Trading and Mining, November 2, 2021

China's Amended Administrative Penalty Law Took Effect on July 15, October 8, 2021

China Issues New Rules Regulating Personal Information Collection by Mobile Apps, April 28, 2021

A New Gateway to China – Recent Policy Developments in the Hainan Free Trade Port, April 6, 2021

China Issues Measures for the Security Review of Foreign Investments, February 9, 2021

China Patent Law Fourth Amendment—Impact on Foreign Companies, January 26, 2021

China Regulators Remove Restrictions on Insurance Fund Investment, December 14, 2020

China Adopts Interim Provisions on the Review of Concentrations of Business Operators for the AntiMonopoly Law, November 30, 2020

China Releases Draft Personal Data Protection Law for Comments, November 12, 2020

China Adopts Export Control Law, November 5, 2020

© 2022 Haynes and Boone, LLP

China Releases New QFII/RQFII Rules, October 27, 2020

China Releases Provisions on Strengthening the Supervision of Private Equity Investment Funds (Draft), October 15, 2020

China Releases Provisions on the Unreliable Entity List, October 5, 2020

China Releases Revised Measures on Handling Complaints of Foreign-Invested Enterprises, September 23, 2020

China Releases Administrative Measures for Strategic Investment by Foreign Investors in Listed Companies, September 10, 2020

China Releases Draft Data Security Law, September 8, 2020

China Releases Circular on Further Stabilizing Foreign Trade and Foreign Investment, August 24, 2020

China Releases Draft Measures for the Administration of Imported and Exported Food Safety, August 18, 2020

U.S. Listed Chinese Companies: Regulatory Scrutiny and Strategic Options, July 30, 2020

China Passes Controversial Hong Kong National Security Law, July 9, 2020

China's Relaxed Financial Sector May Aid Foreign Investors, June 18, 2020

Is There a Law in China Similar to the US Defense Production Act?, May 8, 2020

Coronavirus Brings Force Majeure Claims to LNG Contracts, March 4, 2020

The Rise of China, March 4, 2020

Coronavirus Fears Cast Cloud Over Dealmaking, February 27, 2020

Additional questions? Please contact Haynes Boone lawyers Liza L.S. Mark and Sarah Sheng.

© 2022 Haynes and Boone, LLP